Remarks

Title Change

Please change the title to "User selection of computer login."

Drawings

The replacement drawing sheets comprise deletions of reference numbers from the following figures because the reference numbers were not mentioned in the disclosure: transmission(s) and signal(s) in Fig. 3 & 4; no and yes in Fig. 7 & 8; mouse speed, mouse vector, and key in Fig. 14; no and submission completed? in Fig. 15; signal match, I, key remaining? for each signal, for each remaining key in Fig. 17; key, no, retry, key file, initial key file, wrong key file, terminal key file, first key trajectory, second key trajectory, third key trajectory, last key trajectory, in Fig. 18; key, no, retry, key file, initial key file, wrong key file, terminal key file, first key trajectory, second key trajectory, last key trajectory, in Fig. 19.

35 U.S.C. §102 Prior Art - USPN 6,766,456 (McKeeth)

User Selection

McKeeth anticipated receiving a variety and combination of types of input signals, but never anticipated that a user could select which are to be used for authentication. McKeeth only stated that "the computer system may be designed" or "the computer system may be configured", never suggesting that the user may set the design or configuration used for authentication.

> The system comprises a user interface configured to communicate security information and an implicit input to the computer. [2:8-10]
>
> For example, the computer system 100 may be designed to receive a combination of input signals in a form of a password from a keyboard, in a form of a fingerprint scan from an optical scanner (e.g., placed on the keyboard or mouse), and in a form of a geometric pattern from a mouse or trackball. [3:12-17]

While McKeeth was replete with input variations, there was no suggestion that in McKeeth's system the user made the determination of the input types, not only of device, but especially signal type. To the contrary, McKeeth actually taught away from such signal type user configuration, as

McKeeth relied upon what he called "implicit input": monitoring a preconfigured mandatory signal type. If the user was free to choose the signal types, as claimed by the instant invention herein, there would be no implicit input, and McKeeth's system as disclosed would not have existed.

> In one embodiment, the user is always required to perform an implicit, invisible, or non-apparent act (the "implicit" act or input). The implicit input may include an active and/or a passive act. For instance, in performing the active act, the user may generate a geometric pattern (e.g., using a mouse) when requesting access to the computer system 100. The computer system 100 may be configured to recognize a particular geometric pattern under the condition that the user performs such pattern concurrently with, or after a predetermined duration from, scanning his/her fingerprint. In performing the passive act, the user may wait a predetermined time intervals between entry of various components of the security information or, for instance, may skip a predetermined letter of each component of the security information. In heightened security applications, it may be desirable to configure the computer system 100 to issue a security alert to the responsible authority (e.g., security guards or law enforcement personnel) if the user fails to perform the geometric pattern. Accordingly, even if the compare circuit 150 determines that the input (e.g., fingerprint) and security information do match, the compare circuit 150 may still issue the flag signal because of the user's failure to perform the geometric pattern. [4:5-27]
>
> In such a scenario, the computer system 150 recognizes that while the user may be legitimate, the user's failure to perform the geometric pattern may be an indication that the user is experiencing duress or force to access the computer system 100, as described for the method of FIG. 4. In some applications, it may be desirable to grant a limited access to the user to give the false impression that access to the computer system 100 is granted as usual. As used herein, "limited access" is any access that provides a user or intruder access that is less than complete access to the computer system 100. However, concurrently with the limited access, a silent security alert may be issued to security personnel, without allowing the user or intruder to know. Using the silent security alert mode silent alert minimizes risk to the user under duress. [4:28-43]

The claimed instant invention herein is an improvement upon McKeeth's system, which, under McKeeth's duress example, could be compromised by someone knowing what the set system configuration of implicit input was, or at least knowing if it was not performed. As

claimed, user selection of device and/or signal type provides a combinatorial explosion of possibilities as to what proper user inputs could be.

Iterative Incremental Authentication

In reference to claim 43 regarding iterative incremental authentication, and examiner's previous rejection in that claim area, McKeeth [3:52-4:4] disclosed a fingerprint compare circuit which failed to anticipate iterative incremental authentication. Previously examiner-cited McKeeth [4:5-28], quoted above, disclosed his implicit input idea, something completely different than iterative incremental authentication as presently claimed.